UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTOPHER VICTOR GRUPE,

Defendant.

DEFENDANT'S MOTIONS IN LIMINE

Case No. 17-CR-00090 PJS-DTS

Hon. Patrick J. Schiltz

This case involves highly technical issues involving the functioning of Canadian Pacific Railway's ("CPR") corporate computer network and the functionality of four Cisco Nexus 7000 network switches (the "Cisco Switches") that handled business enterprise data and applications for that network. These four Cisco Switches were configured into two network "boxes" consisting of two switches a piece. One box was located at Canadian Pacific Plaza ("CPP") in Minneapolis, Minnesota, and the other in Ogden, Canada. Additionally, there are complex technical issues revolving around Remote Access Point ("RAP") log ons, Microsoft Active Directory functionality, and computer logs that can only be properly understand through expert testimony. Yet the government, despite repeated requests from the defense, has not noticed any experts as required by Federal Rule of Criminal Procedure 16. It is now the eve of trial, and still the government has provided no expert notices. This raises the concern that the government will improperly attempt to use lay fact witnesses to opine on issues that require qualified expert testimony. This is a significant issue the defense wishes to bring to the Court's attention. Thus, Christopher Victor Grupe, through his counsel, moves this Court in the following Motions in Limine to:

1. Exclude under Federal Rules of Evidence 701 and 702 and Federal Rule of Criminal Procedure 16 any testimony of fact witnesses that reach technical conclusions or other opinions that expert testimony is required for;
2. Exclude the attached documents, offered as indicative examples, produced by the government because, among other issues, they contain improper speculation in the form of lay opinion, hearsay, are fatally incomplete, and violate the Best Evidence Rule. (*See e.g.,* Exs. A & B);
3. Exclude all evidence subject to Federal Rule of Evidence 404(b) as the government has not provided notice of using such evidence at trial after a request by the defense.

BACKGROUND

On April 11, 2017, the government indicted Mr. Grupe, charging a single violation of 18 U.S.C. § 1030(a)(5)(A), under the Computer Fraud and Abuse Act ("CFAA"). (Indictment ,Dkt. 1.) On September 19, 2017, the government superseded the Indictment. (Dkt. 33.) The Superseding Indictment ("SI") makes certain factual changes to the Indictment and adds a reference to the sentencing provision for section 1030(a)(5)(A), section 1030(c)(4)(B)(i). It still charges a single count violation of 18 U.S.C. § 1030(a)(5)(A). This section of the CFAA prohibits the knowing transmission "of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." *See* 18 U.S.C. 1030(a)(5)(A). Furthermore, under the alleged facts, the loss from damage caused to the protected computer must exceed $5,000.00 for Mr. Grupe to be convicted of a felony. *See id.* at (c)(4)(A)(i)(l).

Specifically, the SI charges that Mr. Grupe, as an "IT professional working for Canadian Pacific Railway in Minnesota" accessed Canadian Pacific's computer network on December 17, 2015 and "deleted data, including deleting some system administrator accounts entirely and changing passwords for the other system administrator accounts" and that he attempted to conceal his access to the system. (SI ¶¶ 1, 4 (Dkt. 33).) Count 1 alleges that these actions caused "loss to Canadian Pacific during the period from December 17, 2015 to December 17, 2016, of an aggregate value of more than $5,000.00 . . . ." (*Id.*)

On April 11, 2017, the Court issued a bench warrant for Mr. Grupe. (Dkt. 3). On April 12, 2017, Mr. Grupe voluntarily appeared before this Court and was released on a $25,000 bond with minimal conditions. (*See* Dkts. 3-7.) He has complied with all his conditions of release. Trial is currently scheduled for 9:00 AM on October 2, 2017 with a status conference scheduled for 2:00 PM on September 28, 2017. (Dkts. 28, 32.)

The government is providing Mr. Grupe with discovery on a rolling basis. Much of the discovery provided to date contains, among other issues, speculation constituting improper expert opinion in violation of Federal Rule of Evidence 702, as well as multiple levels of hearsay.

This Motion in Limine does not attach all the government's discovery that the defense finds objectionable, rather it seeks to highlight this crucial issue for the Court at an early stage by moving to exclude from evidence two indicative examples containing opinions that only a qualified expert may offer.

As Motions in Limine are threshold objections that must be renewed at trial, Mr. Grupe does not waive his right to object to any evidence, or make other objections, not detailed in this motion.[1]

ARGUMENT

I. THE COURT SHOULD EXCLUDE ALL SPECULATIVE CONCLUSIONS IN DOCUMENTS AND TESTIMONY ON TECHNICAL ISSUES INVOLVING CANADIAN PACIFIC RAILWAY'S COMPUTER NETWORK AND ASSOCIATED HARDWARE BECAUSE IT REQUIRES EXPERT TESTIMONY AND THE GOVERNMENT HAS NOTICED NO EXPERTS

The government has not noticed any expert to the defense under Fed. R. Crim. P. 16, despite the defense's requests and the highly technical nature of this case. Significant factual and legal questions in this case involve complex technical issues involving advanced computer hardware, such as the workings of CPR's Cisco Nexus 7000-series Network Switches, running both as physical and virtual switches.[2] The discovery produced by the government to date is rife with conclusory statements, all drawn from digitally stored evidence such as computer logs files, about the identity of the perpetrator of the alleged acts, the potential implications of those alleged acts, and the operation of CPR's network that stretch far beyond anything a lay witness is qualified to testify about.

---

[1] *See, e.g., Luce v. United States*, 469 U.S. 38, 41 n. 4 (1984) ("Although the Federal Rules of Evidence do not explicitly authorize in limine rulings, the practice has developed pursuant to the district court's inherent authority to manage the course of trials."); *Estate of Rick v. Stevens*, No. C 00-4144-MWB, 2002 WL 1713301, at *3 (N.D. Iowa July 2, 2002) (quoting *Jonasson v. Lutheran Child & Family Servs.*, 115 F.3d 436, 440 (7th Cir. 1997)). ("Here the district court demonstrated a keen understanding of the proper role and limits of the motion in limine. It ruled on those matters that could be determined as threshold issues and deferred ruling on those matters on which it believed that the interest of both parties would be better served by deferring the ruling until the issue could be determined in a more concrete setting.")

[2] Essentially, a network switch can be viewed as similar to a telephone switchboard in that it connects data from point A to point B, governed by certain rules and procedures, much like a telephone switchboard was used to connect caller A to caller B. *See* https://www.cisco.com/c/en/us/products/switches/nexus-7000-series-switches/index.html?stickynav=1 (Cisco's webpage for the network switches at issue here) (last accessed September 20, 2017).

These opinions require expert testimony. Indeed, many of the statements in the discovery are demonstrably false, and many others present firm certainty based on bare and uncritical speculation. Thus, Mr. Grupe expects a dangerously blurred boundary between permissible lay opinion rationally based on the witnesses' perceptions, but not "scientific, technical, or other specialized knowledge," and impermissible expert opinion to be a major issue in this case. The defense seeks to highlight these issues for the Court pre-trial.[3]

Federal Rule of Evidence 701 states that lay witnesses may only give opinions: (1) rationally based on the witness's perception; (2) helpful to clearly understanding the witness's testimony or to determining a fact in issue; and (3) not based on scientific, technical, or other specialized knowledge within the scope of Federal Rule of Evidence 702.[4] Lay witnesses must have personal knowledge about the subject matter of their testimony,[5] and may only testify to matters within the common knowledge of laypersons or from their experience based on those perceptions.[6] An essential difference between expert and non-expert testimony is that only a qualified expert may answer hypothetical questions.[7]

---

[3] *See* Fed. R. Evid. 701-03.

[4] Fed. R. Evid. 701.

[5] Fed. R. Evid. 602.

[6] *See Khoday v. Symantec Corp.,* 93 F. Supp. 3d 1067, 1085 (D. Minn. 2015), *as amended* (Apr. 15, 2015); *United States v. Peoples*, 250 F.3d 630, 640–41 (8th Cir.2001) (concluding that a police officer should not have been allowed to testify as to the specialized meaning of code words on recorded conversations because she had not been qualified as an expert); *United States v. Ganier*, 468 F.3d 920, 927 (6th Cir. 2006) (citing *United States v. Peoples*, 250 F.3d 630, 640–41 (8th Cir.2001) (holding that the interpretation a lay witness needed to apply to make sense of the software reports was "more similar to the specialized knowledge police officers use to interpret slang and code words used by drug dealers" and that his testimony could only be offered under Rule 702); *United States v. Figueroa-Lopez*, 125 F.3d 1241, 1246 (9th Cir. 1997) ("The mere percipience of a witness to the facts on which he wishes to tender an opinion does not trump Rule 702.")

a. The Government's Discovery Includes Numerous Documents Containing Improper Lay Opinion

Numerous documents in the government's produced discovery contain improper lay opinion, as well as impermissible hearsay. The defense foresees the government's discovery presenting significant evidentiary issues at trial. The defense does not yet know what, if any, of the discovery it has received that the government will attempt to enter into evidence at trial. As examples of these pervasive issues, the defense draws attention to two documents from the government's discovery, Exs. A & B, which the Court should deem inadmissible in their entirety.

b. The Government's Discovery Contains Improper Expert Opinion From Lay Fact Witnesses and All Such Evidence Should Be Excluded

The two attached exhibits from the government's produced discovery are prime examples of documents full of opinions that only a qualified expert may properly testify to at trial.

First, Exhibit A is an Incident Response Report produced by CrowdStrike Professional Services (the "Crowdstrike Report".) By reaching conclusions and stating opinions on the central issues of this case, it is a quintessential example of an expert report.[8]

---

[7] *Hartzell Mfg., Inc. v. Am. Chem. Techs., Inc.,* 899 F. Supp. 405, 408–09 (D. Minn. 1995) (holding that a non-expert witness was not the proper witness to respond to hypothetical facts or circumstances, and was not competent to review documents that were extraneous to business records or his own industry experience merely to have a basis to form opinion testimony.)

[8] Crowdstrike's website is located at https://www.crowdstrike.com/ (last accessed Sept. 20, 2017.)

The Crowdstrike Report purports to reach its conclusions from "triag[ing] one (1) workstation system using Falcon Host; and" using "[l]everaged router logs provided to CrowdStrike by CPR." (*See* Ex. A at Bates No. 00000199, p. 7). It does not explain what it means to "triage" a workstation system using Falcon Host, or what "leveraged" router logs are. It then lays out its conclusory "Key Findings" based on hearsay documents provided by CPR. (*See id.* at Bates No. 00000200, p. 8.) But it does not detail its methods of analysis or the basis of its opinions beyond haphazardly cut-and-pasting the information provided by CPR into a spreadsheet. The report is entirely murky as to methodology or bases for its expert opinions and conclusions on highly technical issues far beyond the province of a lay witness. The CrowdStrike Report, and any testimony related to it, should be excluded in its entirety from the government's case in chief.[9]

Second, Exhibit B is an email chain between CPR executives that includes a conclusory summary from Ernest Seguin. (See Ex. B at Bates No. 00000380-85, pp. 3-8.) Based on the government's discovery the defense expects Mr. Seguin to be the government's key witness. The government has not noticed Mr. Seguin as an expert witness.

Exhibit B, like Exhibit A, is full of opinions that only a qualified expert may testify to. This Court should not allow the government to introduce expert witness testimony or reports in the guise of lay fact witnesses. Thus, the Court should exclude Exhibit B in its entirety and forbid testimony by Mr. Seguin or other lay witnesses offering expert opinions of the types contained in Exhibit B.[10]

---

[9] The defense reserves the right to use anything in the government's production for impeachment purposes.

[10] *See US Salt, Inc. v. Broken Arrow, Inc*., 563 F.3d 687, 690 (8th Cir. 2009) (holding that lay witness's proposed testimony regarding lost profits amounted to speculation because he failed to perform an adequate analysis to support a damage claim for future lost profits).

Exhibit B contains an email dated January 11, 2016, in which Ernest Seguin concludes that "Chris Grupe used his RAP, PC, and cached credentials to login into the CP network under the acct GRU0040. He did so the day after he resigned his position at CP." (Ex. B at Bates No. 00000381, p. 4.) Mr. Seguin later speculates the consequences of Mr. Grupe's alleged conduct, surmising "[i]f an emergency communication problem occurred, CP staff would not be able to fix it." (*See* Ex. B at Bates No. 00000382, p. 5.) Mr. Seguin also states "Above he did successfully copy off the CP critical config DATA." (*See id*.) This vague statement, which fails to offer any meaningful detail or context, is inadmissible opinion testimony, as, for example, only a qualified expert may assess whether data was or was not "critical." Again, when commenting on Mr. Grupe's alleged conduct, Mr. Seguin states that "[a]t this point the railway was at extreme risk." (*See id*.). Mr. Seguin falsely deduces that the alleged conduct would impact rail security,

Admitting this kind of evidence would admit expert testimony under the guise of lay testimony.[11] This would subvert the disclosure requirements of Federal Rule of Criminal Procedure 16 as well as the *Daubert* reliability requirements.[12] Thus, the Defense requests that Mr. Seguin and others be prohibited from testifying on the topics contained within the above-mentioned documents.

II. EXHIBITS A & B CONTAIN INADMISSABLE HEARSAY AND MUST BE EXCLUDED

Exhibits A & B contain multiple out-of-court hearsay statements that should be excluded from trial. The statements in these documents are inadmissible under Federal Rule of Evidence 801. Federal Rule of Evidence 801 defines hearsay as a statement, other

[11] *United States v. Peoples,* 250 F.3d 630, 641 (8th Cir. 2001).

[12] *Id.*

than the one made by the declarant, while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. The Federal Rules of Evidence prohibit the admission of hearsay with very limited exceptions.[13] If there is hearsay within hearsay, each piece of hearsay must individually satisfy an exception to be admissible.[14]

Exhibit A, without identifying the original speaker or providing original source documents, sets forth an "incident response." The report's "key findings" include that the user gru0040 logged into the system. Corresponding alleged log excerpts are attached to the report. These findings are, however, inadmissible hearsay. The report fails to meet any of the established hearsay exceptions, and it is not a business record, as it was not kept in the course of Canadian Pacific's or CrowdStrike's regularly conducted business activity.[15]

Similarly, the statements made in Exhibit B are multilevel hearsay not subject to any exception. Throughout the emails in this document, Canadian Pacific executives and management make statements concerning Mr. Grupe's alleged conduct. The individuals making these statements, however, lack personal knowledge of the conduct alleged, as they were not on-site at the time the conduct is said to have taken place, and several did not personally review the quoted log files or lacked the personal or industry knowledge to speculate as to what those log files show or fail to show. Mike Redeker, for example, states on January 11, 2016 to Laird Pitz that "Chris Grupe, proceeded to make his way though our network and changed key passwords…" This conclusory and damning

[13] Fed. R. Evid. 802.

[14] Fed. R. Evid. 805.

[15] Fed. R. Evid. 803(6).

statement, made with no personal knowledge of any relevant events on December 2015 must be excluded at trial if the government wishes to use it to prove the truth of the matter asserted. This statement is unreliable hearsay that does not fit into any exceptions. Moreover, its legal conclusions concerning Mr. Grupe are improper, as it is the fact finder's duty to determine if defendants violate applicable law.

The emails in Exhibit B contain other statements that conclude Mr. Grupe's culpability prior to the completion of any internal corporate investigation or criminal trial. Significantly, these are all hearsay statements made by individuals the government has not indicated it intends to call at trial. In an email from January 11, 2016 to Mike Redeker, Tim Winn states that the log files and Crowdstrike data identify "what it was that Chris Grupe was doing on December 17th" and that while in some cases Chris accessed the network devices "only to pull a copy of the configurations" "[i]n other cases he went much further." In the final email of the Exhibit, Sergeant Reardon speculates "[s]ounds like [Mr. Grupe] used Cached files on his laptop to do his tampering." (*See* Ex. B, Bates No. 00000378, p. 1).

CONCLUSION

This is a highly technical case involving Canadian Pacific Railway's corporate computer network in Minneapolis, Minnesota and Ogden, Canada. At issue is the alleged access to four Cisco Nexus 7000 computer network switches paired in two locations: one set in Minnesota, and one in Canada. Yet, despite repeated requests from the defense, the government has not noticed any expert witness, despite producing discovery rife with conclusions only a qualified expert may properly make. It is now the eve of trial. The Court should exclude the above documents in Exhibits A and B, and other government exhibits which contain improper expert testimony or that contain the type of impermissible expert opinion the defense anticipates the government will offer in its case in chief. Additionally, given that trial is imminent, the Court should bar the government from noticing any experts at this late hour. The government has had ample time to do so, and has not.

September 20, 2017
Brooklyn, New York

Respectfully submitted,

Frederic B. Jennings
Frederic B. Jennings
(Bar No. 5240679)
Tor Ekeland Law, PLLC
195 Montague Street, 14th Floor
Brooklyn, NY 11201-3631
Tel: (718) 737 7264
Fax: (718) 504 5417
fred@torekeland.com